

On a Furstenberg-Katznelson-Weiss type theorem over finite fields

Le Anh Vinh
 Mathematics Department
 Harvard University
 Cambridge, MA 02138, US
 vinh@math.harvard.edu

July 17, 2008

Abstract

Using Fourier analysis, Covert, Hart, Iosevich and Uriarte-Tuero (2008) showed that if the cardinality of a subset of the 2-dimensional vector space over a finite field with q elements is $\geq \rho q^2$, with $q^{-1/2} \ll \rho \leq 1$ then it contains an isometric copy of $\geq c\rho q^3$ triangles. In this note, we give a graph theoretic proof of this result.

1 Introduction

A classical result due to Furstenberg, Katznelson and Weill ([4]) says that if $E \subset \mathbb{R}^2$ has positive upper Lebesgue density, then for any $\delta > 0$, the δ -neighborhood of E contains a congruent copy of a sufficiently large dilate of every three point configuration. In [3], Covert, Hart, Iosevich and Uriarte-Tuero investigated an analog of this result in finite field geometries. They addressed the case of triangles in two-dimensional vector spaces over finite fields.

Given $E \subset \mathbb{F}_q^2$, where \mathbb{F}_q is a finite field of q elements, define

$$T_3(E) = \{(x, y, z) \in E \times E \times E\} / \sim \quad (1.1)$$

with the equivalence relation \sim such that $(x, y, z) \sim (x', y', z')$ if there exists $\tau \in \mathbb{F}_q^2$ and $O \in SO_2(\mathbb{F}_q)$, the set of two-by-two orthogonal matrices over \mathbb{F}_q with determinant 1, such that

$$(x', y', z') = (O(x) + \tau, O(y) + \tau, O(z) + \tau). \quad (1.2)$$

The main result of [3] is the following (see [3] and the references therein for the motivation and related results to this theorem).

Theorem 1.1 ([3]) *Let $E \subset \mathbb{F}_q^2$, and suppose that*

$$|E| \geq \rho q^2 \quad (1.3)$$

for some $\frac{C}{\sqrt{q}} \leq \rho \leq 1$ with a sufficiently large constant $C > 0$. Then there exists $c > 0$ such that

$$|T_3(E)| > c\rho q^3. \quad (1.4)$$

In this note, we will provide a graph theoretic proof of this result. More precisely, we only give a different proof of the key estimate (Estimate (2.4) in Section 2) in Covert, Hart, Iosevich and Uriarte-Tuero's proof. Our result however is interesting in its own right as it is related to the number of hinges (i.e. paths of length two) in a large subgraph of an (n, d, λ) -graph. The rest of this note is organized as follows. In Section 2, we study the arguments of Covert, Hart, Iosevich and Uriarte-Tuero in [3] and discuss where graph theoretic methods can play a role. In Section 3, we establish a theorem about the number of colored paths of length two in a pseudo-random coloring of a graph. Using this theorem, we will give another proof of Theorem 1.1 in the last section.

2 Covert, Hart, Iosevich and Uriarte-Tuero's arguments

In this section, we follow closely the presentation in [3]. Covert, Hart, Iosevich and Uriarte-Tuero observed that it suffices to show that if $|E| > \rho q^2$, then

$$|\{(a, b, c) \in \mathbb{F}_q^3 : |T_{a,b,c}(E)| > 0\}| \geq c\rho q^3, \quad (2.1)$$

where

$$T_{a,b,c}(E) = \{(x, y, z) \in E \times E \times E : \|x - y\| = a, \|x - z\| = b, \|y - z\| = c\}, \quad (2.2)$$

with

$$\|x\| = x_1^2 + x_2^2.$$

This follows from the following lemma which states that over finite fields, a (non-degenerate) simplex is defined uniquely (up to translation and rotation) by the norms of its edges.

Lemma 2.1 (cf. Lemma 2.1 in [3]) *Let P be a (non-degenerate) simplex with vertices V_0, V_1, \dots, V_k with $V_j \in \mathbb{F}_q^d$. Let P' be another (non-degenerate) simplex with vertices V'_0, \dots, V'_k . Suppose that*

$$\|V_i - V_j\| = \|V'_i - V'_j\| \quad (2.3)$$

for all i, j . Then there exists $\tau \in \mathbb{F}_q^d$ and $O \in SO_d(\mathbb{F}_q)$ such that $\tau + O(P) = P'$.

The key estimate of the proof of Theorem 1.1 in [3] is the following result about hinges.

Theorem 2.2 (cf. Theorem 2.2 in [3]) Suppose that $E \subset \mathbb{F}_q^2$ and let $a, b \neq 0$. Then

$$|\{(x, y, z) \in E \times E \times E : \|x - y\| = a, \|x - z\| = b\}| = |E|^3 q^{-2} + O(q|E|).$$

And if $|E| \gg q^{3/2}$, then

$$|\{(x, y, z) \in E \times E \times E : \|x - y\| = a, \|x - z\| = b\}| = (1 + o(1))|E|^3 q^{-2}. \quad (2.4)$$

Since $|E| \geq \rho q^2$ for some $\frac{1}{\sqrt{q}} \ll \rho \leq 1$, we have $|E| \gg q^{3/2}$. From (2.4), by the pigeon-hole principle, there exists $x \in E$ such that

$$|\{(y, z) \in E \times E : \|x - y\| = a, \|x - z\| = b\}| \geq |E|^2 q^{-2}.$$

We have two cases.

Case 1. Suppose that the number of elements of $SO_2(\mathbb{F}_q)$ that fix x and keep (y, z) inside the pinned hinge is no more than ρq . Since $|E| \geq \rho q^2$, the number of distinct distances c from $\{y \in E : \|x - y\| = a\}$ to $\{z \in E : \|x - z\| = b\}$ is at least

$$|E|^2 q^{-2} \frac{1}{\rho q} \geq \frac{1}{2} \rho q.$$

Since there are $(q - 1)^2$ possible choices for a and b , (2.1) follows.

Case 2. Suppose that the number of elements of $SO_2(\mathbb{F}_q)$ that fix x and keep (y, z) inside the pinned hinge is more than ρq . Then both the circle of radius a , centered at x , and the circle of radius b , centered at x , contain more than ρq elements of E . It is shown that (cf. Lemma 2.3 in [3]) the number of distinct distance c from $\{y \in E : \|x - y\| = a\}$ to $\{z \in E : \|x - z\| = b\}$ is at least $\frac{\rho q}{4}$. Since there are $(q - 1)^2$ possible choices for a and b , (2.1) follows.

Thus the proof of Theorem 1.1 can be reduced to Theorem 2.2. The main purpose of this note is to give a graph theoretic proof of Theorem 2.2.

3 Number of hinges in an (n, d, λ) -graph

We call a graph $G = (V, E)$ (n, d, λ) -graph if G is a d -regular graph on n vertices with the absolute values of each of its eigenvalues but the largest one is at most λ . It is well-known that if $\lambda \ll d$ then an (n, d, λ) -graph behaves similarly as a random graph $G_{n, d/n}$. Precisely, we have the following result (cf. Theorem 9.2.4 in [1]).

Theorem 3.1 ([1]) Let G be an (n, d, λ) -graph. For a vertex $v \in V$ and a subset B of V denote by $N(v)$ the set of all neighbors of v in G , and let $N_B(v) = N(v) \cap B$ denote the set of all neighbors of v in B . Then for every subset B of V :

$$\sum_{v \in V} (|N_B(v)| - \frac{d}{n}|B|)^2 \leq \frac{\lambda^2}{n}|B|(n - |B|). \quad (3.1)$$

The following result is an easy corollary of Theorem 3.1

Theorem 3.2 (cf. Corollary 9.2.5 in [1]) *Let G be an (n, d, λ) -graph. For every set of vertices B and C of G , we have*

$$|e(B, C) - \frac{d}{n}|B||C|| \leq \lambda\sqrt{|B||C|}, \quad (3.2)$$

where $e(B, C)$ is the number of edges in the induced bipartite subgraph of G on (B, C) (i.e. the number of ordered pair (u, v) where $u \in B$, $v \in C$ and uv is an edge of G).

Suppose that a graph G of order n is colored by t colors. Let G_i be the induced subgraph of G on the i^{th} color. We call a t -colored graph G (n, d, λ) -r.c. (regularly colored) graph if G_i is an (n, d, λ) -graph for each color $i \in \{1, \dots, t\}$. The following result gives us an estimate for the number of colored paths of length two in an (n, d, λ) -r.c. graph G .

Theorem 3.3 *Let G be an (n, d, λ) -r.c. graph. For any two colors r, b and every set of vertices E of G , we have*

$$|e_{r,b}(E) - \left(\frac{d}{n}\right)^2 |E|^3| \leq 2\frac{\lambda d}{n}|E|^2 + \lambda^2 |E|, \quad (3.3)$$

where $e_{r,b}(E)$ is the number of (r, b) -colored paths of length two (i.e. the number of ordered triple $(u, v, w) \in E \times E \times E$ with uv, vw are edges of G , uv is colored r and vw is colored b).

Proof For a vertex $v \in V$ let $N_E^r(v)$ and $N_E^b(v)$ denote the set of all r neighbors and b neighbors of v in E , respectively. From Theorem 3.1, we have

$$\begin{aligned} \sum_{v \in E} (|N_E^r(v)| - \frac{d}{n}|E|)^2 &\leq \sum_{v \in V} (|N_E^r(v)| - \frac{d}{n}|E|)^2 \leq \frac{\lambda^2}{n}|E|(n - |E|) \\ \sum_{v \in E} (|N_E^b(v)| - \frac{d}{n}|E|)^2 &\leq \sum_{v \in V} (|N_E^b(v)| - \frac{d}{n}|E|)^2 \leq \frac{\lambda^2}{n}|E|(n - |E|). \end{aligned}$$

Thus, by the Cauchy Schwarz inequality, we have

$$\begin{aligned} &\left[\sum_{v \in E} (|N_E^r(v)| - \frac{d}{n}|E|)(\frac{d}{n}|E| - |N_E^b(v)|) \right]^2 \\ &\leq \left[\sum_{v \in E} (|N_E^r(v)| - \frac{d}{n}|E|)^2 \right] \left[\sum_{v \in E} (|N_E^b(v)| - \frac{d}{n}|E|)^2 \right] \leq \frac{\lambda^4}{n^2}|E|^2(n - |E|)^2. \end{aligned}$$

This implies that

$$\left| \sum_{v \in E} N_E^r(v)N_E^b(v) + \left(\frac{d}{n}\right)^2 |E|^3 - \frac{d}{n}|E| \sum_{v \in E} (N_E^r(v) + N_E^b(v)) \right| \leq \frac{\lambda^2}{n}|E|(n - |E|) \quad (3.4)$$

From Theorem 3.2, we have

$$\left| \sum_{v \in E} N_E^r(v) - \frac{d}{n} |E|^2 \right| \leq \lambda |E| \quad (3.5)$$

$$\left| \sum_{v \in E} N_E^b(v) - \frac{d}{n} |E|^2 \right| \leq \lambda |E|. \quad (3.6)$$

Putting (3.4), (3.5) and (3.6) together, we have

$$\left| \sum_{v \in E} N_E^r(v) N_E^b(v) - \left(\frac{d}{n} \right)^2 |E|^3 \right| \leq 2 \frac{\lambda d}{n} |E|^2 + \frac{\lambda^2}{n} |E| (n - |E|) < 2 \frac{\lambda d}{n} |E|^2 + \lambda^2 |E|, \quad (3.7)$$

completing the proof of the theorem. \square

If we color an (n, d, λ) -graph by one color then Theorem 3.3 becomes.

Theorem 3.4 *Let G be an (n, d, λ) -graph. For every set of vertices E of G , we have*

$$|p_2(E) - \left(\frac{d}{n} \right)^2 |E|^3| \leq 2 \frac{\lambda d}{n} |E|^2 + \lambda^2 |E|, \quad (3.8)$$

where $p_2(E)$ is the number of ordered paths of length two in E (i.e. the number of ordered triple $(u, v, w) \in E \times E \times E$ with uv, vw are edges of G). In particular, if $|E| \gg \lambda \left(\frac{n}{d} \right)$ then the number of ordered paths of length two in E is

$$(1 + o(1)) |E|^3 \left(\frac{d}{n} \right)^2. \quad (3.9)$$

Remark 3.5 *Using the second moment method, it is not difficult to show that for every constant p the random graph $G(n, p)$ contains*

$$(1 + o(1)) p^r (1 - p)^{\binom{s}{2} - r} \frac{n^s}{|\text{Aut}(H)|} \quad (3.10)$$

induced copies of H . Alon extended this result to (n, d, λ) -graphs. He proved that every large subset of the set of vertices of a (n, d, λ) -graph contains the “correct” number of copies of any fixed small subgraph (Theorem 4.10 in [5]).

Theorem 3.6 ([5]) *Let H be a fixed graph with r edges, s vertices and maximum degree Δ , and let $G = (V, E)$ be an (n, d, λ) -graph, where, say, $d \leq 0.9n$. Let $m < n$ satisfies $m \gg \lambda \left(\frac{n}{d} \right)^\Delta$. Then, for every subset $U \subset V$ of cardinality m , the number of (not necessarily induced) copies of H in U is*

$$(1 + o(1)) \frac{m^s}{|\text{Aut}(H)|} \left(\frac{d}{n} \right)^r. \quad (3.11)$$

Note that, in the “simple case”, H is a path of length two, then Theorem 3.6 is weaker than Theorem 3.4.

4 Graph theoretic proof of (2.4)

Let \mathbb{F}_q denote the finite field with q elements where $q \gg 1$ is an odd prime power. For a fixed $a \in \mathbb{F}_q^*$, the finite Euclidean graph $G_q(a)$ in \mathbb{F}_q^2 is defined as the graph with vertex set \mathbb{F}_q^2 and the edge set

$$E = \{(x, y) \in \mathbb{F}_q^2 \times \mathbb{F}_q^2 \mid x \neq y, \|x - y\| = a\},$$

where $\|\cdot\|$ is the analogue of Euclidean distance $\|x\| = x_1^2 + x_2^2$. In [6], Medrano et al. studied the spectrum of these graphs and showed that these graphs are asymptotically Ramanujan graphs. They proved the following result.

Theorem 4.1 ([6]) *The finite Euclidean graph $G_q(a)$ is regular of valency $q \pm 1$ for any $a \in \mathbb{F}_q^*$. Let λ be any eigenvalues of the graph $G_q(a)$ with $\lambda \neq$ valency of the graph then*

$$|\lambda| \leq 2\sqrt{q}. \quad (4.1)$$

Now consider the set of colors $L = \{c_1, \dots, c_{q-1}\}$ corresponding to elements of \mathbb{F}_q^* . We color the complete graph $G_q = K_{q^2}$ with vertex set \mathbb{F}_q^2 by $q - 1$ colors such that $(x, y) \in \mathbb{F}_q^2 \times \mathbb{F}_q^2$ is colored by the color c_i if $\|x - y\| = i$. Then from Theorem 4.1, G_q is a $(q^2, q \pm 1, 2\sqrt{q})$ -r.c. graph. Estimate (2.4) follows immediately from Theorem 3.3.

Remark 4.2 *Note that the conclusion of (2.4) holds with the Euclidean norm $\|\cdot\|$ is replaced by any non-degenerate quadratic form on \mathbb{F}_q^2 . This fact can be shown similarly as the above. Let Q be a non-degenerate quadratic form on \mathbb{F}_q^2 . The finite Euclidean graph $E_q(Q, a)$ is defined as the graph with vertex set \mathbb{F}_q^2 and the edge set*

$$E = \{(x, y) \in \mathbb{F}_q^2 \times \mathbb{F}_q^2 \mid x \neq y, Q(x - y) = a\}. \quad (4.2)$$

In [2], Bannai, Shimabukuro and Tanaka studied the spectrum of the graph $E_q(Q, a)$ and showed that these graphs are asymptotically Ramanujan graphs.

Theorem 4.3 ([2]) *Let Q be a non-degenerate quadratic form on \mathbb{F}_q^2 . The finite Euclidean graph $E_q(Q, a)$ is regular of valency $q \pm 1$ for any $a \in \mathbb{F}_q^*$. Let λ be any eigenvalues of the graph $E_q(Q, a)$ with $\lambda \neq$ valency of the graph then*

$$|\lambda| \leq 2\sqrt{q}. \quad (4.3)$$

Similarly, consider the set of colors $L = \{c_1, \dots, c_{q-1}\}$ corresponding to elements of \mathbb{F}_q^* . We color the complete graph $G_q = K_{q^2}$ with vertex set \mathbb{F}_q^2 by $q - 1$ colors such that $(x, y) \in \mathbb{F}_q^2 \times \mathbb{F}_q^2$ is colored by the color c_i if $Q(x - y) = i$. Then from Theorem 4.1, G_q is a $(q^2, q \pm 1, 2\sqrt{q})$ -r.c. graph. From Theorem 4.3 and Theorem 3.3, we are done.

Acknowledgments

The research is performed during the author's visit at the Erwin Schrödinger International Institute for Mathematical Physics. The author would like to thank the ESI for hospitality and financial support during his visit.

References

- [1] N. Alon and J. H. Spencer, *The probabilistic method*, 2nd ed., Willey-Interscience, 2000.
- [2] E. Bannai, O. Shimabukuro and H. Tanaka, Finite Euclidean graphs and Ramanujan graphs, *Discrete Mathematics* (to appear).
- [3] D. Covert, D. Hart, A. Iosevich and I. Uriarte-Tuero, An analog of the Furstenberg-Katznelson-Weiss theorem on triangles in sets of positive density in finite field geometries, preprint (2008).
- [4] H. Furstenberg, Y. Katznelson and B. Weiss, Ergodic theory and configurations in sets of positive density, Mathematics of Ramsey Theory, 184-198, *Algorithms Combi.*, **5**, Springer, Berlin (1990).
- [5] M. Krivelevich and B. Sudakov, Pseudo-random graphs, *Conference on Finite and Infinite Sets Budapest*, Bolyai Society Mathematical Studies X, pp. 1–64.
- [6] A. Medrano, P. Myers, H. M. Stark and A. Terras, Finite analogues of Euclidean space, *Journal of Computational and Applied Mathematics*, **68** (1996), 221–238.